



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/049,264

09/30/2002

Katsuyuki Okeya

500.41178 X00

9433

24956

7590

06/13/2006

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.  
1800 DIAGONAL ROAD  
SUITE 370  
ALEXANDRIA, VA 22314

EXAMINER

POLTORAK, PIOTR

ART UNIT

PAPER NUMBER

2134

DATE MAILED: 06/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No. 10/049,264	Applicant(s) OKEYA, KATSUYUKI	
	Examiner Peter Poltorak	Art Unit 2134	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 4/13/05.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-30 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☒ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |                                                                                                                                                       |                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                                                           | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                                                  | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>2/11/02, 4/13/05</u> . | 6) <input type="checkbox"/> Other: _____                                                |

### DETAILED ACTION

1. Claims 1-30 have been examined.

#### *Priority*

2. Acknowledgment is made of applicant's claim for foreign priority based on an application filed in Japan (2000-345457 on 11/08/2000 and 2000-393279 on 12/21/2000 and PCT/JP01/09781 on 11/08/01).

It is noted, however, that applicant has not filed an original and certified copy of the Japanese application as required by 35 U.S.C. 119(b).

#### ***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. The claimed invention is directed to non-statutory subject matter. Claims 1-23 and 26-30 are essentially directed to an arithmetic system and a method, the steps are not defined in such a way that they could not be implemented without the use of computers, e.g. implemented by utilizing pens and paper. As a result, the claims refer to abstract ideas.
4. Furthermore, in order to meet the requirement of patentability, software must be embodied on computer readable media. Claim 26 does not disclose what type of medium stores the program "related" in claims 1 to 20. As a result storage media such as paper, a human mind etc. read on claim 26. As a result, claims 1-20 are directed towards abstract ideas. Also, given the lack of clarity of the relationship (see

term: "related" used in claim 26) between claims 1-20 and 26, it is unclear whether claim 26 is directed towards the apparatus or the method.

5. Lastly, the claims do not provide any tangible results. An attempt is noted in claims 22 and 23; however, the claims only mention signature and decrypting data in the preambles, while missing some steps that would result in a tangible outcome, e.g. generating a signature that is used in authentication etc. The decryption method does not provide any decryption steps.

### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1-30 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that applicant regards as the invention.
7. The claims are generally narrative and indefinite, failing to conform with current U.S. practice. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors. Especially the "transforming" and "calculating" steps and phrases such as: "a point on an elliptic curve in the elliptic curve".

8. Claims 1-25, 27-30 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of steps, such omission amounting to a gap between the necessary structure. See MPEP 2172.01.
9. The omitted structural cooperative relationships are: the "calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve" that never happens. Similarly, neither data nor signature cited in claims 21-22 is generated. In fact these claims are missing some essential steps. Claim 23 has the same problem as claims 21-22.
10. Claim 26 is not understood. The claim recites: "program relating to the scalar multiplication method according to any one of claims 1-20". It is not clear what kind of relationship is intended.
11. The term: "complete coordinate" is not understood especially since the recited coordinate does not seem to necessarily be the coordinate on the recited elliptic curve.

Appropriate correction is required.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

12. Claims 1-3 are rejected under 35 U.S.C. 102(a) as being anticipated by Blake (Blake, Seroussi & Smart "Elliptic Curves in Cryptography", ISBN: 0521653746, Jan. 2000).

Blake discusses the use of elliptic curves in cryptography.

13. As per claims 1-3 Blake discloses calculating partial information of a scalar-multiplied point (pg. 35-37), and a step of recovering a complete coordinate (in affine and in projective coordinates) from the partial information of said scalar-multiplied point (Blake, pg. 41-42 and 57-60).

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

14. Claims 4-13, 21-24 and 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blake (Blake, Seroussi & Smart "Elliptic Curves in Cryptography", ISBN: 0521653746, Jan. 2000) in view of Johnson (Johnson and Menezes, "The Elliptic Curve Digital Signature Algorithm (ECDSA)", Feb. 2000).

Blake elliptic curve teaching has been discussed above. As per claims 4-7 pages 57-60 read on giving X-coordinate and Z-coordinate of said scalar-multiplied point as the partial information of said scalar-multiplied point in projective\affine coordinates and X-coordinate and Z-coordinate of a point obtained by adding said scalar-multiplied point and the point on the elliptic curve in the projective/affine coordinates.

The examiner points out that adding negative values results in subtraction. Similarly the division is essentially a process of subtraction.

15. Blake does not explicitly recite Weierstrass or Montgomery form elliptic curve being used in the steps recited above but using these curves in the above application would have been an obvious modification given the fact that they are well known and successfully used in the cryptographic encryptions (see Blake pg. 29 or Okeya pg. 241 and 244-245 for example). Similarly, using affine coordinates or projective coordinate at particular steps would have been an obvious modification of each other. Utilizing any of these coordinates is well known as and successfully used in the elliptic curve calculation as disclosed by Blake.

16. As per claims 21-24 and 26-28 Blake does not explicitly teach digital signature generation, encryption/decryption of data and using a computer apparatus with a storage medium.

Johnson discloses generation of a digital signature (Johnson, pg. 24-25). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize elliptic curve steps disclosed by Blake in order to generate a digital signature as taught by Johnson given the benefit of entity authentication and non repudiation. Digital signature involves encryption/decryption of data and using a computer apparatus to generate and verify signature is implicit as well as storing programs performing the steps on the computer storage medium.

17. As per claims 8-13 public key cryptography (which includes elliptic curve computation as disclosed by Johnson) involves encryption and decryption and these steps are obvious variants of one another.

### ***Conclusion***

Blake (Blake, Seroussi & Smart "Elliptic Curves in Cryptography", ISBN: 0521653746, Jan. 2000) in view of Johnson (Johnson and Menezes, "The Elliptic Curve Digital Signature Algorithm (ECDSA)", Feb. 2000) discloses Weierstrass-form/Montgomery-form elliptic curve transformation. However, Blake does not provide motivation to combine the teaching with the previously cited art. As a result the limitations as recited in claims 14-20, 25 and 29-30 overcome the art of record. However, claims 14-20, 25 and 29-30 must overcome the 35 USC § 101 and 112 rejections in order to be considered for allowability.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

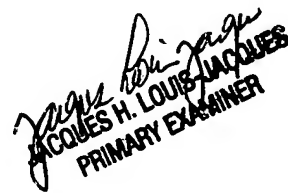
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis Jacques can be reached on (571)272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.



Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



6/9/06

  
JACQUES H. LOUIS  
PRIMARY EXAMINER